NANCI L. CLARENCE (State Bar No. 122286)
EDWIN K. PRATHER (State Bar No. 190536)
CRAIG H. BESSENGER (State Bar No. 245787)
CLARENCE & DYER LLP
899 Ellis Street
San Francisco, California 94109
Telephone: 415.749.1800
Facsimile: 415.749.1694
Email: nclarence@clarencedyer.com
eprather@clarencedyer.com
cbessenger@clarencedyer.com

Attorneys for Defendant Jeffrey Harrison

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

UNITED STATES OF AMERICA,

Plaintiff,

v.

JEFFREY HARRISON,

Defendant.

Case No. CR-07-0594 PJH

NOTICE OF MOTION AND MOTION TO SUPPRESS EVIDENCE; REQUEST FOR EVIDENTIARY HEARING; MEMORANDUM OF POINTS AND AUTHORITIES IN SUPPORT OF MOTION TO SUPPRESS

Date: March 5, 2008
Time: 2:30 p.m.
Judge: Hon. Phyllis J. Hamilton

TO: JOSEPH RUSSONIELLO, UNITED STATES ATTORNEY, AND DENISE BARTON, ASSISTANT UNITED STATES ATTORNEY:

Please take notice that on Wednesday, March 5, 2008, at 2:30 p.m. or as soon thereafter as this matter may be heard, defendant Jeffrey Harrison will and hereby does move to suppress all evidence derived from the unlawful search of his computer and other electronic storage devices conducted on July 1, 2007. Alternatively, Mr. Harrison requests an evidentiary hearing at which he may present and develop further evidence in support of such motion. This motion is based on the Fourth Amendment to the United States Constitution, the memorandum of points and authorities, the pleadings filed in this action, all applicable constitutional, case, and statutory authority, and such other evidence and argument as the court may take notice.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

FEDERAL CASES

FEDERAL STATUTES & REGULATIONS

STATE STATUTES

MISCELLANEOUS

MEMORANDUDM OF POINTS AND AUTHORITIES

INTRODUCTION

This motion presents the court with a unique question, as yet not faced by the federal courts, which strikes at the core of the American legal system and the ability of lawyers to represent their clients and discharge their professional duties and obligations.

Jeffrey Harrison is a 62-year-old attorney, licensed to practice law in California. An accomplished trial lawyer, Mr. Harrison also worked as an executive officer of a telecommunications company, Global Mobile Technologies (GMT), based in Singapore with offices in the Philippines. In addition to providing legal counsel to GMT, Mr. Harrison was in the process of representing GMT's Chief Technology Officer, Donald Stern, in multiple ongoing lawsuits in California. On July 1, 2007, Mr. Harrison returned to San Francisco from a business trip to the Philippines. Due to the nature of his work with GMT, as well as his legal representation of Mr. Stern, Mr. Harrison traveled with privileged and confidential legal information stored on a laptop computer and CD-R's[1].

At San Francisco International Airport, a Customs agent decided to search the information stored on the computer in Mr. Harrison's possession. The Customs agent had been informed that Mr. Harrison was an attorney, and Mr. Harrison protested that the computer contained privileged and confidential legal information. The Customs agent ignored Mr. Harrison's entreaties and searched the information stored on the computer. Federal agents then used information obtained from this search to interrogate Mr. Harrison, and to extract statements from him. This motion seeks to suppress all of the information retrieved from Mr. Harrison's computer, CD-R's, and any other electronic storage devices searched, as well as all evidence obtained directly and indirectly as a result of that information, including Mr. Harrison's statements, as the fruits of a violation of Mr. Harrison's rights under the Fourth Amendment to the United States Constitution.[2]

---

[1] A CD-R is a "compact disc-recordable," a small polycarbonate disc that can have data "written" or recorded onto it by the laser in some compact disc drives.

[2] *See, e.g., Mapp v. Ohio*, 367 U.S. 643 (1961) (evidence obtained in violation of Constitution cannot be used at trial against criminal defendant in state or federal court); *Wong*

The fruits of this unreasonable search must be suppressed. A Ninth Circuit District Court has already held that border searches of any traveler's computer must be justified by reasonable suspicion because of the privacy and dignity interests invaded by such a search.[3] Mr. Harrison, by virtue of his professional obligations as an attorney, had a heightened expectation of privacy in the information stored on his computer and CD-R's. Mr. Harrison's heightened privacy interest in the digital contents of his computer and CD-R's rendered their search inherently intrusive and "non-routine." The searches were not justified by any objective, articulable, reasonable level of suspicion, and thus violated the Constitution's Fourth Amendment.

The ubiquitous use of computers and other electronic devices to store and manage confidential attorney-client material is not simply a problem created by lawyers, to be solved by lawyers. To the contrary, "As society grows ever more reliant on computers as a means of storing data and communicating, courts will be called upon to analyze novel legal issues and develop new rules within our well-established Fourth Amendment jurisprudence."[4] The safeguard of reasonable suspicion to conduct such a search must be applied here in order to protect the privacy interests of attorneys in their digitally stored information. To hold otherwise – to hold that suspicionless border searches of attorneys' computers are permissible under the Constitution – would tell attorneys they have absolutely no expectation of privacy in the digital content of their computers and other electronic storage devices when they travel. Such a holding would not only jeopardize the sanctity of attorney-client privileged materials, it would place every attorney in an untenable ethical quandary at this country's border.

Sun v. United States, 371 U.S. 471 (1963) (evidence obtained by exploiting initial unconstitutional activity, without resort to a distinguishable independent basis, must be suppressed). The fruits of the unconstitutional computer search at SFO include all contraband seized, and any statements made by Mr. Harrison, during and after the raid on his home. The facts establishing probable cause for the warrant authorizing the raid consist entirely of evidence obtained from Mr. Harrison's computer at SFO and from his subsequent interrogation. *See* Affidavit of Michael J. Appio at pp. 11-14, a true and correct copy of which is attached hereto as Exhibit A. Mr. Harrison did not consent to the search of his home. *Id.* at p. 13.

[3] *United States v. Arnold*, 454 F. Supp. 2d 999, 1000-01 (C.D. Cal. 2006), *appeal argued*, No. 06-50581 (9th Cir. Oct. 18, 2007).

[4] *United States v. Adjani*, 452 F.3d 1140, 1152 (9th Cir. 2006).

STATEMENT OF FACTS

On July 1, 2007, Mr. Harrison returned to the United States from a business trip to the Philippines. Declaration of Jeffrey Harrison ("Harrison Decl.") at ¶ 2, a true and correct copy of which is attached hereto as Exhibit B.[5] Admitted to the State Bar of California in 1971, Mr. Harrison is an accomplished trial attorney who in recent years has focused on working with technology companies. Harrison Decl. at ¶ 4. Mr. Harrison traveled to Asia frequently in his role as the Chief Executive Officer of Global Mobile Technologies (GMT), a company based in Singapore with offices in the Philippines. *Id.* at ¶ 3. In addition to providing legal counsel to GMT, Mr. Harrison individually represented GMT's Chief Technology Officer, Donald Stern, in ongoing lawsuits in California. *Id.* at ¶ 5. The lawsuits included actions for patent infringement and fraud. *Id.* at ¶ 5. Mr. Harrison had many attorney-client privileged conversations with his client, Mr. Stern, as they worked on Mr. Stern's legal matters during this trip to the Philippines. Declaration of Donald Stern ("Stern Decl.") at ¶ 3, a true and correct copy of which is attached hereto as Exhibit C. Mr. Harrison stored privileged and confidential legal information related to his ongoing matters on a laptop computer and CD-R's that he carried with him on business trips. Harrison Decl. at ¶ 6.

Unless otherwise indicated, the following facts are based on a collective report, prepared by various U.S. Customs officers. Customs and Border Patrol Report ("CBP Report"), a true and correct copy of which is attached hereto as Exhibit D. The report, written entirely in the third person, consists of a compilation of statements apparently written at various times and attributed to various Customs agents involved in Mr. Harrison's detention and search. It is unclear when the agents entered the various sections they contributed to the report. Crucial portions of the statements in this collective report are unsupported by any raw notes or other contemporaneously recorded information produced to the defense.

Mr. Harrison's return flight to this country landed at San Francisco International Airport

---

[5] In connection with Mr. Harrison's declaration and possible testimony in support of this motion, *see Simmons v. United States*, 390 U.S. 377, 394 (1968).

(SFO). CBP Report at p. 1. In SFO's luggage retrieval area, Customs and Border Patrol (CBP) officer Matthew Moran approached Mr. Harrison and "referred him for a secondary CBP baggage examination" because of his "demeanor and his frequent travel to a high risk area." *Id.* at p. 3. CBP officer Moran claims Mr. Harrison, a U.S. citizen just arrived home after a lengthy flight from Asia, "appeared to be angry that he was selected for a basic interview." *Id.* at p. 3; Harrison Decl. at ¶ 2. Mr. Harrison also allegedly "avoided eye contact" and had shaky hands, which CBP officer Moran interpreted as "signs of nervousness." CBP Report at p. 3.

In the secondary inspection area, CBP officer Edwards "proceeded to ask Harrison about the details of his trip." *Id.* at p. 1. In response, Mr. Harrison "stated that he traveled to the Philippines for 10 days on a business trip" and that "he is the owner of Global Mobile Technologies LLP." *Id.* at p. 1. In the course of discussing his trip to the Philippines, Mr. Harrison also told CBP officer Edwards that he was an attorney and explained the nature of his legal work. Harrison Decl. at ¶ 8.

CBP officer Edwards searched all of Mr. Harrison's luggage. *Id.* at ¶¶ 7, 9. Contrary to the CBP report, no other CBP officer searched Mr. Harrison's belongings in his presence. *Id.* at ¶ 7. According to the CBP report, "Due to the fact that Harrison was returning from a country which is considered high risk for child sex tourism and child pornography, CBPO Edwards felt it was appropriate to review the numerous amounts of media (CD-R, laptop, jump drives, digital camera) in [Harrison's] possession." CBP Report at p. 1. CBP officer Edwards asked Mr. Harrison for his computer. Harrison Decl. at ¶ 9. Mr. Harrison informed CBP officer Edwards that the computer had confidential and attorney-client privileged legal files on it and that she could not search it. *Id*. at ¶ 9. In response, CBP officer Edwards told Mr. Harrison that he could not object to the computer's search. *Id*. at ¶ 9. Mr. Harrison handed over his computer bag, which held his computer and a number of CD-R's. *Id*. at ¶ 9. Mr. Harrison gave the computer bag to CBP officer Edwards, *not* CBP officer Cross as the CBP report asserts. *Id.* at ¶ 9. After taking the computer out of its bag, CBP officer Edwards turned the computer on. *Id.* at ¶¶ 9, 10. Once the computer booted up, CBP officer Edwards asked Mr. Harrison for the log-on password. *Id.* at ¶ 10. Mr. Harrison refused to disclose the password, telling CBP officer Edwards that the

computer contained privileged and confidential legal files. Harrison Decl. at ¶ 10. It was only after CBP officer Edwards informed Mr. Harrison again that he could not object to the computer's search that Mr. Harrison revealed the computer's password. *Id.* at ¶ 10.

CBP officer Edwards searched the information on Mr. Harrison's computer for some time. *Id.* at ¶ 11. She then gathered the computer and its carrying bag, which held multiple CD-R's, and began to leave the inspection area. *Id.* at ¶ 11. The report claims that "[a]s CBPO Edwards attempted to go review the CD-R's on the CBP computer in the main office, Harrison started following CBPO Edwards and belligerently stating that the CD-R's were his personal belongings and CBP could not review while not in his presence." CBP Report at p. 2. In fact, Mr. Harrison repeated to CBP officer Edwards that the computer and CD-R's contained privileged and confidential legal information that CBP officer Edwards could not review. Harrison Decl. at ¶ 12. In response, "CBPO Edwards explained to Harrison that all items in his possession were subject to inspection including all media." CBP Report at p. 2. CBP officer Edwards then "went into the main office to review the CD-R's because that is the only area where to view [sic] the CD-R's." *Id.* at p. 2.

Some time later, CBP officer Edwards "contacted [Immigration and Customs Enforcement (ICE) Special Agent (SA)] Appio and described the nature of the images found." *Id.* at p. 3. In response, "SA Appio confirmed that he would respond to review the images and interview the subject." *Id.* at p. 3. Before ICE SA Appio interviewed Harrison, "CBPO Edwards requested a pat down to insure that Harrison was not concealing any other media devices in his clothing or on his person. . . . [T]he pat down was conducted by CBPO Moran . . . with negative results." *Id.* at p. 3. Mr. Harrison was then "turned over to ICE SA Appio for an interview" during which Mr. Harrison allegedly made incriminating statements[6], which the defense now seeks to suppress. *Id.* at p. 3.

[6] The facts are not sufficiently developed at this time to determine the adequacy of any *Miranda* advisement, thus Mr. Harrison reserves the right to move to suppress statements on these grounds pending an evidentiary hearing on this matter.

ARGUMENT

I. Border Searches of Computers and Other Electronic Storage Devices Violate the Fourth Amendment Unless Supported By Reasonable Suspicion

a. The Fourth Amendment's Protections Extend to Border Searches

The Fourth Amendment protects "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." U.S. Const. amend. IV. To protect this right, the Fourth Amendment demands that most searches and seizures be authorized by a warrant based on probable cause. *Illinois v. Gates*, 462 U.S. 213, 236 (1983). A narrow exception to the Fourth Amendment's warrant requirement exists at the country's border, however, based on the United States' "inherent sovereign authority to protect its territorial integrity. By reason of that authority, it is entitled to require that whoever seeks entry must establish the right to enter and to bring into the country whatever he may carry." *Torres v. Puerto Rico*, 442 U.S. 465, 473 (1979).

The Fourth Amendment still applies at the border, however, limiting the government's authority to search travelers and their possessions by ensuring that such searches are reasonable. *United States v. Villamonte-Marquez*, 462 U.S. 579, 588 (1983). Thus the oft-quoted line that "searches made at the border . . . are reasonable simply by virtue of the fact that they occur at the border," when taken out of context, elides the fact that the Fourth Amendment's protections remain in effect during border searches. *United States v. Ramsey*, 431 U.S. 606, 616 (1977) (holding that border searches do not require probable cause and a warrant to be reasonable). Indeed, the Court in *Ramsey* stated that border searches are still "subject to substantive limitations imposed by the Constitution . . . ." *Id.* at 620. The Supreme Court has reiterated this Constitutional limitation on border searches, at times tacitly – there would be no need for the Court's extensive border search jurisprudence if all such searches were inherently reasonable – and more concretely. *United States v. Montoya de Hernandez*, 473 U.S. 531, 539 (1985) ("Having presented herself at the border for admission . . . respondent was entitled to be free from unreasonable search and seizure.")

Under the border search exception to the Fourth Amendment's warrant requirement,

therefore, "*[r]outine* searches of the persons and effects of entrants are not subject to any requirement of reasonable suspicion, probable cause, or warrant . . . ." *Montoya de Hernandez*, 473 U.S. at 538 (emphasis added). Non-routine border searches, in contrast, are unreasonable unless supported by some level of articulable suspicion. *United States v. Okafor*, 285 F.3d 842, 846 (9th Cir. 2002). For purposes of the border search exception, an international airport terminal is the functional equivalent of a border. *Almeida-Sanchez v. United States*, 413 U.S. 266, 272-73 (1973). Thus, as the Ninth Circuit recently held, "passengers deplaning from an international flight are subject to routine border searches." *United States v. Romm*, 455 F.3d 990, 996 (9th Cir. 2006).

b. Border Searches of Computers Are Inherently Invasive and Non-Routine

The only published decision in the Ninth Circuit to squarely address the standard applicable to border searches of electronic storage devices held such searches are non-routine and that "the correct standard requires that any border search of the information stored on a person's electronic storage device be based, at a minimum, on reasonable suspicion." *United States v. Arnold*, 454 F. Supp. 2d 999, 1001, 1003 (C.D. Cal. 2006), *appeal argued*, No. 06-50581 (9th Cir. Oct. 18, 2007) (suppressing evidence of child pornography on traveler's electronic storage devices because search of devices not supported by reasonable suspicion).[7] The *Arnold* decision is the controlling law in the Ninth Circuit and both its facts and reasoning are on all fours with the search of Mr. Harrison's computer and other devices.

In *Arnold*, the 43-year-old defendant arrived at LAX after a long flight from the Philippines. *Id.* at 1001. After retrieving his luggage, Arnold proceeded to customs and was selected for secondary questioning. *Id.* A CBP officer asked Arnold where he had traveled, for how long, and the purpose of his trip. *Id.* Arnold responded that he had been on vacation for

---

[7] *Arnold*'s reasonable suspicion standard applies only to searches of information stored on electronic devices, not searches for physical contraband smuggled within them. 454 F. Supp. 2d at 1007. Thus, border agents need no suspicion before requiring a traveler to turn on a computer or subjecting it to an X-ray machine in order to determine whether the physical space of the computer contains a bomb, drugs, or other contraband. Such a search implicates different interests. A traveler does not have a substantial *privacy* interest in the internal physical space of a computer, which properly should contain only circuit boards, batteries, processors, and the like.

three weeks visiting friends. *Id.* The CBP officer then inspected Arnold's luggage and discovered Arnold's computer. *Id.* After having Arnold turn on the computer, CBP officers searched its files and discovered a photo of two nude women. *Id.* A further search by ICE agents uncovered images of suspected child pornography. *Id.*

Arnold filed a motion to suppress, arguing that the search of his computer's files was non-routine and not supported by reasonable suspicion. *Id.* at 1000. The court in *Arnold* agreed, and suppressed the challenged evidence. *Id.* at 1001. In reaching its holding, the *Arnold* court observed that:

> While not physically intrusive as in the case of a strip or body cavity search, the search of one's private and valuable personal information stored on a hard drive or other electronic storage device can be just as much, if not more, of an intrusion into the dignity and privacy interests of a person. This is because electronic storage devices function as an extension of our own memory. . . . Therefore, government intrusions into the mind – specifically those that would cause fear or apprehension in a reasonable person – are no less deserving of Fourth Amendment scrutiny than intrusions that are physical in nature.

454 F. Supp. 2d at 1000-01.

Although the court noted in support of its analysis that "[a]ttorneys' computers may contain confidential client information," its decision did not rely on the necessity of protecting an attorney's heightened privacy interest in such privileged and confidential information. *Id.* at 1004. In the *Arnold* court's analysis, the privacy and dignity interests of *any* traveler in her electronically-stored information are sufficient to render a border search of that information "substantially more invasive than a search of the contents of a lunchbox or other tangible object." *Id.* at 1003, 1004.

No federal court of appeals has contradicted *Arnold* entirely by holding border searches of the information on computers and other devices are categorically routine. While every court of appeals to address such border searches has affirmed the challenged search, each court has done so in the context of overwhelming and patent factual evidence of criminal behavior supporting the search, rendering moot the issue of whether the government needs reasonable suspicion to conduct such searches.

The Ninth Circuit has held that the search of a computer's information falls within the border-search exception, but explicitly avoided addressing whether such a search is routine or non-routine. *United States v. Romm*, 455 F.3d 990, 997 n.11 (9th Cir. 2006) (Canada refused entry to defendant, a convicted sex offender on probation, based on his criminal record and his confession to visiting child pornography websites; defendant's computer searched at U.S. border after Canadian officials contacted U.S. Customs agents).

The Fifth Circuit evaluated the outbound border search of computer diskettes as non-routine and affirmed the search based on the existence of reasonable suspicion, without deciding whether such searches are routine or non-routine. *United States v. Roberts*, 274 F.3d 1007, 1014, 1016 (5th Cir. 2001) (Customs agents received information from local law enforcement that the defendant would be boarding an international flight at a particular airport, on a particular day, carrying child pornography saved on diskettes stored in his shaving kit).

The Fourth Circuit, in an opinion drowning in expansive dicta, held only that 19 U.S.C. § 1581(a) authorized the border search of a computer and computer disks, that the particular challenged search was reasonable for Fourth Amendment purposes, and denied a challenge to the search on First Amendment grounds. *United States v. Ickes*, 393 F.3d 501, 505, 507 (4th Cir. 2005) (Customs agents "discovered marijuana paraphernalia, photo albums of child pornography, a disturbing video focused on a young ball boy, and an outstanding warrant for [the defendant's] arrest" and then searched a computer and disks).

The Second Circuit affirmed the border search of computer diskettes and undeveloped film only after concurring that the search was supported by reasonable suspicion and explicitly avoided deciding if the search was routine or non-routine. *United States v. Irving*, 452 F.3d 110, 124 (2d Cir. 2006) (computer diskettes searched because defendant was subject of a criminal investigation into sex tourism to Mexico, a convicted pedophile, returning from a visit to a Mexican orphanage, and had children's books and drawings in his luggage).

Unlike the *Arnold* court's decision, none of the appellate court decisions set forth above grappled seriously with the unique nature of searches of electronically stored information, and whether such searches must be supported by reasonable suspicion. The courts avoided reaching

this issue because in each instance the challenged search was supported by a considerable level of objective and articulable reasonable suspicion.[8] That was not the case in *Arnold*, nor is it the case here.

c. No Objective, Articulable Suspicion Existed to Support the Search of Mr. Harrison's Computer and CD-R's

Reasonable suspicion is determined by examining the "totality of the circumstances" for the existence of a "particularized and objective basis for suspecting legal wrongdoing." *United States v. Bravo*, 295 F.3d 1002, 1008 (9th Cir. 2002) (internal quotations omitted). Of course, a determination of reasonable suspicion "must be based upon 'the degree of suspicion that attaches to particular types of non-criminal acts.'" *United States v. Rodriguez*, 976 F.2d 592, 594 (9th Cir. 1992), *quoting United States v. Sokolow*, 490 U.S. 1, 10 (1989). In reviewing a finding of reasonable suspicion, courts "must not accept what has come to appear to be a prefabricated or recycled profile of suspicious behavior very likely to sweep many ordinary citizens into a generality of suspicious appearance merely on hunch." *Rodriguez*, 976 F.2d at 595-96.

Here, since Mr. Harrison deplaned from an international flight, his search occurred at the functional equivalent of the border. According to the CBP Report, CBP officer Edwards made the decision to search Mr. Harrison's electronic storage devices. CBP officer Edwards "felt it was appropriate" to search the information on Mr. Harrison's computer and other devices because Mr. Harrison was returning from the Philippines. She provides no other reason in her report to justify the search of Mr. Harrison's electronic storage devices. Granted, the government may consider the Philippines to be a high risk country for child sex tourism and child pornography. But visits to such a country do not amount to a particularized and objective basis for reasonably suspecting legal wrongdoing.

Basing the invasive search of Mr. Harrison's computer and other storage devices on such

---

[8] *See United States v. Chaudhry*, 424 F.3d 1051, 1055 (9th Cir. 2005) (Fletcher, J. specially concurring) ("[B]ecause there is ample suspicion in each case, it is difficult for judges to consider the issue cleanly on an unencumbered record. Evidence of probable criminal activity . . . cannot help but color judges' views of the facts. We inevitably think 'harmless error.'")

limited information is acting on a hunch, at best. There was no allegation that Mr. Harrison's trip had been paid for in cash, was inexplicably brief, had been carried out for a nonsensical reason, nor of any other facts about his travel that could give rise to objective and articulable reasonable suspicion. *See United States v. Gonzalez-Rincon*, 36 F.3d 859, 863 (9th Cir. 1994) (reasonable suspicion based on, *inter alia*, defendant traveling from source country for narcotics, purchasing ticket with cash on day of trip, carrying single piece of luggage for 15-day trip, and providing inconsistent explanations for trip's purpose).

Mr. Harrison was asked for, and provided, a detailed and truthful explanation for his trip to the Philippines – he was the CEO of a company with offices there. This assertion was corroborated by business cards and other documentation in his possession. Mr. Harrison's trip to the Philippines, therefore, was proof of nothing more than that he had traveled to the Philippines. *See United States v. Romero*, 71 F. Supp. 2d 1021, 1025 n.7 (N.D. Cal. 1999) ("[T]he government attempted to compare the agent's discovery of the $3000 [during a border search] with the discovery of . . . drug paraphernalia . . . . This comparison is barely worthy of response. The possession of drug paraphernalia is evidence that the suspect is engaging in guilty conduct; the possession of money is evidence that the suspect possesses money."). The profile of a "traveler returning from the Philippines" or even "a male traveler returning from the Philippines" – the totality of CBP officer Edwards' stated basis for the computer search at issue – is so broad and general as to inevitably include many innocent citizens within its definition.

Based on *Arnold*'s holding, and the narrower and more compelling ground that Mr. Harrison as an attorney had a heightened expectation of privacy in the privileged and confidential legal materials stored on his electronic devices, the government needed at least reasonable suspicion to justify the challenged searches. The fact that Mr. Harrison traveled to the Philippines cannot reasonably support the government's search of his computer and other electronic storage devices containing attorney-client privileged and confidential legal files. The government did not have the objective and articulable reasonable suspicion it needed to conduct the contested search.

II. Border Searches of Attorneys' Computers Containing Privileged Legal Material Are Profoundly Intrusive and Must Be Supported By Reasonable Suspicion

a. A Border Search Is Unreasonable When the Search's Intrusion Into An Individual's Protected Interests Outweighs the Government's Justification For the Search

The border search of Mr. Harrison's property – the search of an attorney's electronic storage devices containing privileged and confidential information – presents a factual scenario that has apparently never been addressed by the federal courts in this country.[9] Although this court can affirm the *Arnold* court's holding and apply its reasonable suspicion standard to the search at hand, Mr. Harrison's case can also be decided on the much narrower grounds of the search of an attorney's computer and other electronic storage devices. Such a search raises all of the concerns inherent in the search of any traveler's computer, in conjunction with an attorney's vastly heightened expectation of privacy created by her attorney-client privileged materials and work product.[10] As the *Arnold* court held, "[T]o conduct a search of this type without reasonable suspicion goes well beyond the goals of the customs statutes and the reasonableness standard articulated in the Fourth Amendment." 454 F. Supp. 2d at 1007.

Several statutes authorize Customs officers to conduct border searches, including 19 U.S.C.A. § 1467 (West 2008), which reads in part:

> Whenever a vessel from a foreign port or place . . . arrives at a port or place in the United States . . . the appropriate customs officer for such port or place of arrival may, under such regulations as the Secretary of the Treasury may prescribe and for the purpose of

---

[9] A thorough review uncovered no federal case addressing the border search of an attorney's computer. One civil case, *United States v. Modes*, addresses the border seizure of hardcopy attorney-client privileged documents, and applies a reasonable suspicion standard in analyzing the seizure. 787 F. Supp. 1466 (Ct. Int'l Trade 1992) (exclusionary rule applied because government sought quasi-criminal penalties). In *Modes*, a Customs official had sufficient suspicion to visually inspect the nature of a briefcase's contents for evidence of any violation. *Id.* at 1475. During the inspection, the Customs agent was informed the briefcase contained privileged legal files that she could not examine. *Id.* at 1473. Although the initial inspection yielded no evidence of any manner of violation, a Customs supervisor decided to seize the privileged files. *Id*. Based on the lack of evidence of any violation, the court held that no "justifiable and reasonable suspicion" existed to support the seizure. *Id.* at 1475.

[10] Some of these concerns are relevant also to a First Amendment challenge to border search practices, which Mr. Harrison reserves.

> assuring compliance with any law, regulation, or instruction which the Secretary of the Treasury or the Customs Service is authorized to enforce, cause inspection, examination, and search to be made of the persons, baggage, and merchandise discharged or unladen from such vessel . . . .

The reasonableness of a border search is determined by examining the scope of the intrusion, the manner of its conduct, and the justification for its initiation. *See United States v. Duncan*, 693 F.2d 971, 977 (9th Cir. 1982). Although the case law does not always state the analysis in such terms, the balancing of a search's intrusiveness (in scope and manner) against the justification for such intrusion informs all border search decisions. *United States v. Vance*, 62 F.3d 1152, 1156 (9th Cir. 1995) ("As the [border] search becomes more intrusive, more suspicion is needed."); *United States v. Asbury*, 586 F.2d 973, 976 (2d Cir. 1978) ("[R]easonableness is determined by weighing the warranted suspicion of the border official against the offensiveness of the intrusion."); *United States v. Brown*, 499 F.2d 829, 833 (7th Cir. 1974) ("What is required to be balanced in any particular case is the level of suspicion of the agent against the level of indignity perpetrated upon the traveler."). Thus a "routine" border search is simply a search that is so unintrusive in its scope and manner of being conducted as to require no justification for its initiation. Indeed, "a critical factor in distinguishing between routine and non-routine searches" is the level of intrusiveness posed by the search. *United States v. Ramos-Saenz*, 36 F.3d 59, 61 (9th Cir. 1994). [11]

In evaluating border searches of the person, the Ninth Circuit's decisions reflect a continuum whereby the more intrusive a search, the stronger the suspicion necessary to justify it. *Vance*, 62 F.3d at 1156. Even a pat-down search at the border, a relatively *de minimis* intrusion, requires at least some "minimal suspicion." *Id.*; *United States v. Dorsey*, 641 F.2d 1213, 1218 (7th Cir. 1981) ("[S]ome suspicion is required to conduct a patdown [sic] search at the border

---

[11] The statement in *Ramos-Saenz* that "[the Ninth Circuit's] cases hold that a border search goes beyond the routine only when it reaches the degree of intrusiveness present in a strip search or body cavity search," read in context, is not a holding, but rather an incomplete shorthand summary of border search precedent. 36 F.3d at 61. Under Ninth Circuit precedent, pat-down searches at the border require some articulable suspicion to conduct, and therefore are not routine, given that routine border searches may be conducted absent any suspicion at all. *See Vance*, 62 F.3d at 1156.

. . . ."); *United States v. Klein*, 592 F.2d 909, 912 (5th Cir. 1979) (applying "reasonable suspicion" analysis to border pat-down search). A strip search at the border requires "real suspicion." *Vance*, 62 F.3d at 1156. A body-cavity search at the border demands a "'clear indication' that the suspect is carrying contraband in a body cavity." *United States v. Couch*, 688 F.2d 599, 604 (9th Cir. 1982) (*quoting United States v. Aman*, 624 F.2d 911, 912-13 (9th Cir. 1980)).

In parsing searches of objects at the border, the courts have struggled to achieve the nuance evident in evaluating searches of the person because – unlike the readily determined privacy and dignity interests of a person in her body – an individual's protected interests in objects and places searched vary depending on what is being searched. *See United States v. Flores-Montano*, 541 U.S. 149, 152 (2004). Searches of luggage, contents of pockets, and purses are routine and require no level of suspicion. *Vance*, 62 F.3d 1152, 1156. X-ray examinations of luggage and other containers at the border are routine searches. *Okafor*, 285 F.3d at 845-46. To date, the analysis of whether an object's search is non-routine, in other words so invasive in scope or manner as to require some level of suspicion to justify, has turned largely on whether the search is destructive. *Flores-Montano*, 541 U.S. at 154-55. When faced with clear privacy and dignity interests in the thing searched, however, the courts have required some level of suspicion to support the search. *See United States v. Alfonso*, 759 F.2d 728, 738 (9th Cir. 1985) (border search of a ship's living quarters requires more than "naked suspicion").

b. Attorneys Have A Heightened Expectation of Privacy In the Contents of Their Computers Based On Their Professional Duties and Obligations To Clients and the Legal System

With the exception of the decision in *Arnold*, the circumscribed border search jurisprudence described above – focused on restricting physical invasions of the person and destruction of property – has struggled to keep pace with the privacy and dignity interests implicated by searches of the information stored on laptop computers, thumbdrives, CD-R's, and other electronic storage devices with vast capacities. What these two strains of border search analysis fail to adequately address are the vast scope of the intrusion inherent in searches of the information on electronic storage devices and the highly invasive and inconvenient manner in

which the searches are conducted. Only a limited number of published federal criminal cases have analyzed border searches of information on electronic storage devices, and none have been faced – as this court is – with the privacy interests created by the wholly invisible yet profoundly important rights and privileges that may attach to the legal files stored on those devices.

To be clear, Mr. Harrison's motion is not premised on a violation of the attorney-client privilege or the work-product doctrine, although such violations may have occurred here.[12] The existence of the privileged and protected information on Mr. Harrison's computer and other devices contributed to his reasonable expectation of privacy, but that specific information need not be searched in order for the privacy interest to be invaded. As the Supreme Court held in *Arizona v. Hicks*, "[i]t matters not that the search uncovered nothing of any great personal value to respondent – serial numbers rather than (what might conceivably have been hidden behind or under the equipment) letters or photographs. A search is a search, even if it happens to disclose nothing but the bottom of a turntable." 480 U.S. 321, 325 (1987) (lifting a turntable in respondent's home constituted a search and thus violated respondent's expectation of privacy in his home). The government's intrusion into Mr. Harrison's well-founded expectation of privacy occurred as soon as the Customs agent began reviewing the information stored on Mr. Harrison's computer.

In defining the contours of an attorney's privacy interest in the information on a computer containing legal files, it must be recognized that the attorney-client privilege is the oldest testimonial privilege protecting confidential communications, dating to at least the era of Elizabeth I. EDNA SELAN EPSTEIN, THE ATTORNEY-CLIENT PRIVILEGE AND THE WORK-PRODUCT DOCTRINE (4th ed., American Bar Association 2001). The privilege's "seal of secrecy" is "founded upon the necessity, in the interest and administration of justice, of the aid of persons having knowledge of the law and skilled in its practice, which assistance can only be safely and readily availed of when free from the consequences *or the apprehension of* disclosure." *Hunt v.*

---

[12] Mr. Harrison did not directly observe the searches of his computer and other storage devices, thus he does not know whether the government violated these privileges and protections.

Blackburn, 128 U.S. 464, 470 (1888) (emphasis added). In more recent times, the Supreme Court has observed that "if the client knows that damaging information could more readily be obtained from the attorney following disclosure than from himself in the absence of disclosure, the client would be reluctant to confide in his lawyer and it would be difficult to obtain fully informed legal advice." *Fisher v. United States*, 425 U.S. 391, 403 (1976). In California, attorneys are required by statute to "maintain inviolate the confidence, and at every peril to himself or herself to preserve the secrets, of his or her client." CAL. BUS. & PROF. CODE § 6068(e)(1) (West 2008).

The work-product doctrine's protections are equally clear and important. An unjustified effort to obtain an attorney's work product "falls outside the arena of discovery and contravenes the public policy underlying the orderly prosecution and defense of legal claims. Not even the most liberal of discovery theories can justify unwarranted inquiries into the files and the mental impressions of an attorney." *Hickman v. Taylor*, 329 U.S. 495, 510 (1947). The California Rules of Professional Conduct make clear that Business and Professions Code section 6068 applies equally to attorney work product and observe that, "A member's duty to preserve the confidentiality of client information involves public policies of paramount importance." CAL. RULE OF PROFESSIONAL CONDUCT 3-100, discussion 1, 2.

It is in the face of centuries-old privileges forming the bedrock of our legal system that the government, through its practice of suspicionless border searches, equates rifling through an attorney's computer with asking that attorney to empty out the contents of his pockets. Neither search, per current Customs policy, requires an iota of suspicion to conduct. Even granting the lesser expectation of privacy at the border[13], an attorney's privacy interest created by her electronically-stored legal data requires application of the reasonable suspicion standard. In the universe of border search jurisprudence, even a simple pat-down search requires *some* level of suspicion to support it. The search of a ship's living quarters (notably not a physical invasion of the person), requires *some* level of suspicion to support it because of the inherent privacy interests invaded by such a search. It makes no sense for an attorney's privileged materials to be subject to

[13] *Montoya de Hernandez*, 473 U.S. at 539-40.

suspicionless searches.

The privacy interests implicated by the search of an attorney's computer or other device containing privileged files are so substantial that such a search falls closer, in terms of intrusiveness, to a body-cavity search than it does to either a pat-down or living-quarters search. And yet, at the moment, the search and seizure of an attorney's computer is conducted as "routinely" as opening a suitcase and rummaging through one's clothing. Such a search policy is fundamentally flawed. Validating the suspicionless border search of an attorney's computer is the equivalent of telling attorneys that searches of their computers are less of an intrusion on their Fourth Amendment rights than 10-second pat-down searches.

c. An Attorney's Computer Is Not the Simple Equivalent of a Briefcase

The *Arnold* court observed correctly that a traveler's privacy and dignity interests in the information stored on a computer or other device make the search of that information considerably different from the search of a typical closed container. 454 F. Supp. 2d at 1003. The very act of storing information on a computer is different from writing it on a piece of paper and creates a greater expectation of privacy in that information – stored digitally, it is hidden from plain view, and may even be password protected or encrypted. An attorney's reasonable expectation of privacy in legal documents is therefore heightened when they are saved on a computer or other device. An attorney's expectation of privacy in information stored on her computer or other device is not merely subjective, of course. For California-licensed attorneys such as Mr. Harrison, it is objectively supported by statute and other rules of professional conduct governing attorneys, which mandate that attorneys protect client confidences. *See*, *e.g.*, CAL. BUS. & PROF CODE § 6068(e)(1) (West 2008).

The State Bar of California already has addressed issues raised by electronic legal documents. The State Bar's Committee on Professional Responsibility and Conduct issued a formal opinion concluding that electronic versions of documents are included within the definition of "the client papers and property," to which the client is entitled. Formal Op. No. 2007-174 (2007) at p. 4, *available at* http://calbar.ca.gov/calbar/pdfs/ethics/2007-174.pdf. Moreover, the opinion explicitly notes that electronic metadata may reflect a client's confidential

information, which attorneys are obligated to protect under Business and Professions Code section 6068(e)(1). *Id.* at p. 5. Upon request, an attorney is ethically obligated to provide the client with electronic versions of email correspondence, pleadings, deposition and exhibit databases, and other files. *Id.* at p. 4. Attorneys are required, however, to remove metadata relating to other clients before turning over electronic documents. *Id.* at p. 5.

No longer just "glorified typewriters," computers function today as "postal services, playgrounds, jukeboxes, dating services, movie theaters, daily planners, shopping malls, personal secretaries, virtual diaries, and more." Orin Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 569 (2005). Attorneys, in particular, use their computers as virtual law offices, containing entire case files, and have a commensurate expectation of privacy in them. Indeed, "[f]or most people, their computers are their most private spaces." *United States v. Gourde*, 440 F.3d 1065, 1077 (9th Cir. 2006) (en banc) (Kleinfeld, J. dissenting).[14]

While the search of electronically-stored information is invasive due to its broad scope, the manner in which such a search is conducted is also intrusive. The government's analysis of a computer enables it to uncover files the computer's user has affirmatively deleted, which could include drafts of documents and unsent personal or professional correspondence. In addition, computers contain searchable information of which the computer's owner may not even be aware. Kerr, 119 HARV. L. REV. at 542 ("Computers are also remarkable for storing a tremendous amount of information that most users do not know about and cannot control."). The existence of this information on computers subject to search by the government belies the notion that a computer search is the equivalent of viewing hardcopy versions of every document saved on the computer.

The risk of disclosure of client confidences stored on an attorney's computer is heightened by the fact that the government seizes computers at the border without providing their

[14] Judge Kleinfeld's dissent includes an admonition that is especially relevant in the present context of suspicionless border searches of computers, "[s]ex with children is so disgusting to most of us that we may be too liberal in allowing searches when the government investigates child pornography cases. The privacy of people's computers is too important to let it be eroded by sexual disgust." *Gourde*, 440 F.3d at 1078.

owners with any explanation for such seizures. *See* Joe Sharkey, *To Do List: Rename Laptop Files 'Grandma's Favorite Recipes'*, N.Y. TIMES, November 7, 2006, at C6 (hereinafter "Sharkey") ("[A]necdotal evidence indicates a growing number of laptops are being randomly and legally scrutinized, and some are even being seized without a reason given by customs agents when travelers return to the United States."). Such a suspicionless seizure of an attorney's computer poses a grave threat to the duty to preserve client confidences. As one commentator has observed:

> If the government could search and seize privileged communications, attorney-client communications would be severely chilled and lawyers' ability to represent their clients would be undermined. Conscientious attorneys would advise their clients that the government could lawfully intercept their communications. Faced with such a possibility, few clients would feel free to communicate openly with their attorneys.
>
> This chilling effect is unlikely to be eliminated by explaining to clients that their intercepted communications cannot be introduced into evidence at trial.

Eric D. McArthur, Comment, *The Search and Seizure of Privileged Attorney-Client Communications*, 72 U. CHI. L. REV. 729, 738 (2005).

Under current practices, the government *does* search and seize privileged communications at the border, with no justification given. In the face of suspicionless border searches and seizures, clients cannot trust that their confidences are safe with their attorneys, because even a well-founded assertion of privilege will not halt the search of the computer or its impoundment. The potential repercussions are profound. Pending deals or patents could be jeopardized. Trial preparation materials could be lost. The mere specter of such a search and seizure chills an attorney's ability to practice law effectively and undermines confidence in the integrity of our legal system.

d. Attorneys Cannot Fulfill Their Professional Obligations and Duties Unless Their Computers Are Protected From Suspicionless Border Searches

Permitting Customs officers to continue their current practice of suspicionless computer searches at the border places every attorney in an untenable ethical quandary and undermines the public's confidence in the integrity of the legal framework that purports to protect client

confidences. At present, every time an attorney travels internationally with a laptop computer or other device containing privileged and confidential information, that attorney (and that attorney's clients) must be apprehensive that the government might decide to search the putatively protected information for no reason. Under current border search practices, an attorney cannot guarantee, as he or she is statutorily required to do, that the clients' confidences will be maintained inviolate.

An attorney cannot even protect her reasonable expectation of privacy in her computer's digital information during a suspicionless border search by refusing to provide Customs officers with the computer's password, because the computer presumably will be seized. *See* Sharkey, N.Y. TIMES, November 7, 2006, at C6. Thus, in exchange for attempting to discharge her professional obligations, that attorney would be deprived of potentially crucial legal files and forced to abrogate her duty to protect client confidences. Moreover, once the government seizes the computer, the password will not protect the computer's contents from a search. *See United States v. Andrus*, 483 F.3d 711, 719 (10th Cir. 2007) (software used by law enforcement to conduct computer searches "allows user profiles and password protection to be bypassed").

On the other hand, an attorney such as Mr. Harrison, who attempts to avoid the baseless seizure of his computer, will be compelled to disclose its password, thereby granting the government access to its information and surrendering dominion over his legal files and ability to protect his clients' confidences. A search policy is unsound when it poses such a Hobson's choice and undermines the integrity of the duty to maintain privilege. The application of such a policy of suspicionless searches is inherently unreasonable and violates the Constitution's Fourth Amendment.

These dilemmas would be resolved by recognizing that a border search of an attorney's digitally stored information is fundamentally invasive and requires the support of reasonable suspicion, just as other types of invasive border searches already do. A reasonable suspicion requirement will prevent the chilling of an attorney's ability to represent clients effectively because it would guarantee that client confidences and secrets are free from suspicionless invasion by the government. The government already has recognized the chilling effect of suspicionless border searches of information in other contexts and has acted accordingly. *See* 19

C.F.R. § 145.3 (West 2008) (Customs inspectors cannot open sealed mail appearing to contain more than correspondence unless reasonable cause exists to suspect the presence of merchandise or contraband and cannot read correspondence without a warrant or written authorization from the sender or addressee).

e. Requiring Reasonable Suspicion to Search An Attorney's Computer At the Border Will Not Burden or Hinder Law Enforcement

Reasonable suspicion is a low threshold, merely a "'particularized and objective basis for suspecting legal wrongdoing.'" *Bravo*, 295 F.3d at 1008 (quoting *United States v. Arvisu*, 534 U.S. 266 (2002)). Implementing such a minimal standard to support searches of attorneys' computers will not prevent Customs agents from intercepting wrongdoers. As the facts in *Romm*, *Roberts*, *Ickes*, and *Irving* (*supra*) amply demonstrate, professionally trained Customs agents are readily capable of developing facts constituting a basis for reasonable suspicion. Nor will requiring reasonable suspicion for searches of attorneys' computers impose a great logistical burden on law enforcement agents at the border. The number of travelers to whom this protection will apply is a tiny fraction of international passengers, all of whom are regulated and licensed by their respective state bars.

Moreover, there is no reason to believe that implementing a reasonable suspicion standard will suddenly convert attorneys into the smuggler's ally of choice. The sad reality of digital contraband, be it child pornography or a terrorist's attack plan, is that it does not need to be physically carried across the border. Such contraband can be, and most likely is, simply emailed into the country or downloaded from the internet.[15] Given the pervasive quality of the internet, it beggars belief to argue that a reasonable suspicion standard to search attorneys' computers at the

---

[15] As the *Arnold* court recognized, the pervasive nature of digital contraband must also be factored into the balancing of the government's interest in stopping contraband at the border – which justifies the government's heightened authority to search – with the invasion of privacy necessary to effectuate that interest. 454 F. Supp. 2d at 1007. Digital contraband, unfortunately, is not physical and finite. Unlike narcotics, for example, smugglers need not carry digital contraband into this country. The internet, by and large, is the avenue by which digital contraband is imported. In the Fourth Amendment calculus, therefore, while searching computers at the border is a relatively ineffective means of stemming the importation of digital contraband, such searches inevitably require substantial and concrete invasions of privacy.

border will imperil national security or otherwise increase the flow of digital contraband into the country.

While the special concerns and issues inherent to searches of attorneys' computers are critical to the administration of justice, such concerns are not novel. Indeed, the Department of Justice has issued a manual, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*, which contains guidance on searches of computers containing privileged documents and strategies for reviewing privileged computer files. Computer Crime and Intellectual Property Section, Criminal Division, United States Department of Justice, July 2002, *available at* http://www.usdoj.gov/criminal/cybercrime/s&smanual2002.htm#. The government manual warns, in part, that:

> Agents must exercise special care when planning a computer search that may result in the seizure of legally privileged documents . . . . [A]gents should make sure that the search will not violate the Attorney General's regulations relating to obtaining confidential information from disinterested third parties. Second, agents should devise a strategy for reviewing the seized computer files following the search so that no breach of a privilege occurs.

Id. at (II)(B)(7).

The logic behind these guidelines clearly carries over to the border context. Unfortunately, no such safeguards are in place at the border to govern searches of computers and other devices storing privileged and confidential legal material. With the articulation of a reasonable suspicion standard governing such searches, the government will simply be required to develop guidelines to ensure the standard is followed and legally privileged materials are adequately protected. The Department of Homeland Security is empowered to promulgate Customs regulations not related to customs revenue functions. 19 C.F.R. § 0.2 (West 2008).

////

////

////

////

CONCLUSION

The United States has an unquestionable interest in policing its borders and preventing the importation of contraband into the country. That interest, though strong, has substantive limits imposed by the Constitution. These limits are enforced to protect travelers from governmental intrusions into their bodies, their property, and their minds. The government's authority to conduct border searches developed in a time before the internet recast the notion of "borders" and how information crossed them, before digital storage devices enabled average citizens to carry enormous amounts of personal, confidential, and sometimes privileged information with them as they traveled. The *Arnold* court recognized this sea change and implemented a reasonable suspicion standard in border searches of all computers and other devices, a standard that already protects travelers from other types of intrusive searches.

Although *Arnold* clearly governs here, the narrower factual scenario of the search of an attorney's computer has more significant implications than the search addressed in *Arnold*. If in the past attorneys traveled with privileged documents, the documents consisted of paper and ink, and any contraband sought to be found in the attorney's possession was physical and finite. Such contraband, by its nature, could be detected without violating the privileges and protections that are the very underpinnings of this country's legal system. We live in a different time. An attorney's computer or other storage device contains quantities and types of information, and is used in such a manner, as to create expectations of privacy different in kind from anything that has come before.

The law must catch up with the reality of how the government is exerting its power at the border, relying as the government does on outmoded notions of the types of contraband sought and the means employed to search. The government cannot be permitted to conduct suspicionless border searches of an attorney's computer and other electronic storage devices containing privileged and confidential legal files.

///

///

///

Based on the foregoing reasons, Mr. Harrison respectfully requests that the Court find the challenged searches violated the Fourth Amendment and suppress all evidence arising from them. Alternately, Mr. Harrison asks that the Court set an evidentiary hearing so that the defendant may present and develop further facts in support of this motion.

Dated: February 1, 2008

Respectfully submitted,

__/s/: Craig H. Bessenger_____
CRAIG H. BESSENGER
Clarence & Dyer LLP
Attorneys for Jeffrey Harrison